



ケーススタディ

Irwin Mitchell LLP



概要

業界

- ・ 法律

課題

- ・ APTを含む脅威の防御
- ・ クライアントのデータと秘密の保護
- ・ 変化する脅威の先を行く対応

利点

- ・ これまでに知られていないネットワーク内の異常を検出
- ・ トータルなネットワーク可視性
- ・ クライアントのデータの秘匿と保全に対する信頼性の向上
- ・ リアルタイムにインシデントを調査し再現する能力
- ・ 事後対応ではなく変化する状況をコントロールする能力

ビジネスの背景

1912年に設立されたIrwin Mitchellは英国内の大手法律事務所上位20社に入り、英国内に11か所のオフィスを展開しています。2,400名を超える従業員を有するIrwin Mitchellは「フルサービス型」法律事務所であり、個人クライアントおよび企業向けの幅広い法務サービスを、個人、企業、慈善事業、各種団体および組織に対して提供しています。業界において数々の賞を受賞しているIrwin Mitchellは卓越したサービスとイノベーションを高く評価されているこの分野のリーダーです。

“Darktraceは、脅威をより早期に、また発生とともに検知することが可能です。”

Mark Vivian, Head of IT Security at Irwin Mitchell

課題

Irwin Mitchellは長年に渡り、自社のデータシステム、とりわけクライアントの情報の保全を最優先としてきました。特に、ネットワークの動きについてより良く理解し、予期しないイベントがもし発生していればそれがどこかを特定することにより、サイバー脅威の可能性や疑わしいインシデントについて早期に検知する能力を改善したいと希望していました。

Irwin Mitchellは最終的に、もしシステム内で何か異常が発生した場合、その状況がエスカレートする前に対処し、リスクを確実に緩和したいと望んでいたのです。

解決策

サイバーセキュリティ市場を徹底して調査した結果、Irwin MitchellはDarktraceのEnterprise Immune Systemテクノロジーの試用を決めました。「最初にこの製品を見た時、実際に機能するのかどうか懐疑的でした。なぜなら他の製品とあまりにも違っていただけからです。」Irwin MitchellのITセキュリティ責任者、Mark Vivian氏はこのように述べています。「Darktraceと話し合い、デモを見た結果、実際何ができるのか見てみることにしました。それでPOVを実施したのです。」

「インストールと設定は30分程度で済んでしまいました。」Mark Vivian氏はこのように語りました。数週間うちに、DarktraceはIrwin Mitchellのネットワークとユーザーについてきわめて洞察に富んだ情報を提供するのに十分な学習を行いました。」

ケンブリッジ大学で研究された教師なし機械学習および確率論数学に基づき、Enterprise Immune Systemは各ユーザー、デバイスおよびネットワークの「生活パターン」を形成し、「通常」と見なされる動作からのわずかな逸脱も検出することができます。特定の脅威やデータ環境に対する事前の知識を何ら必要とすることなく、自己学習型の Enterprise Immune System は組織の活動を自動的にモデル化し、学習した結果の関連付けを行って絶え間なく判断を改良していきます。

「一部の結果が出始めたところで、私達のシステムが侵害されていないことに確信を持つことができました。一方で、Darktraceを使うことにより、以前に把握されていなかったシステム上のいくつかの設定や処理上の問題を見つけ出すこともできました。」POVにより、Enterprise Immune Systemはその高度な検出機能、ネットワークの100%可視化、調査能力によりビジネスに真の価値を提供できることが実証されました。

POVを終え、Irwin Mitchellは事前対応型のサイバーセキュリティ戦略の主要なコンポーネントとして自社のネットワークへEnterprise Immune Systemを導入し、アクティビティの監視と分析に使用することを決めました。

利点

「サイバーセキュリティは最早"あれば望ましい"ものではなく、必須要件です。そしてクライアントの情報だけでなく、自らの情報も保護しなければなりません。サイバー保険と ISO 27001:2013は必要条件の基準になりつつありますが、それだけでは十分とは言えません。Darktraceは私達がサイバーセキュリティに自信を持っている証となります。監視、警告、調査を、ネットワークの一部のエリアではなく、全体に対して行っているためそう言えるのです。」

ネットワークアクティビティを100%可視化するネットワーク調査インターフェイスであるDarktraceのThreat Visualizerを使って、Irwin MitchellはDarktraceをデータの保全と保護のための全体的なインテリジェンスツールとして使用するだけでなく、アプリケーションサポートから原因分析まで幅広い用途に活用しています。

Threat Visualizerは調査対象となる異常やインシデントを指摘するだけでなく、脅威の深刻度に応じて自動的に分類も行います。これにより、混雑したネットワークの雑音の中でも、ある時点で最も重要な問題に即座に集中することが可能になります。また、Darktraceはインシデントのリアルタイムでの監視に加えて、再生機能も提供しています。これにより詳細な調査を実施して特定のインシデントの発生した状況を理解することが可能になります。

「ネットワークをリアルタイムで見ることはもちろん便利ですが、いつでも任意の時点に戻って再生できる機能は当社にとって非常に大きな変革を意味しています。」Mark Vivian氏はこのように述べています。「私にとって、実際に何が起きているかを理解できることは非常に大きなメリットでした。」

脅威がますます高度化する環境において、Irwin MitchellはEnterprise Immune Systemの自動学習機能を活用し、新しい問題に先手を打つことで、自社およびクライアントの重要資産保護の信頼性を向上させています。ネットワークや脅威の変化に惑わされることなく、Irwin Mitchellはセキュリティに対して先進的かつ積極的なスタンスで対応することが可能となりました。

Darktraceについて

世界経済フォーラムにて“テクノロジー・パイオニア”に選出されたDarktraceは、世界をリードするサイバー防御企業の1つです。DarktraceのEnterprise Immune System技術は、ケンブリッジ大学で開発された機械学習と数学理論をベースに、組織内のあらゆるデバイス、ユーザおよびネットワークの動作を分析し、これまでに特定されていない脅威をリアルタイムに検出します。エネルギーおよび公益事業、金融サービス、ヘルスケア、電気通信、製造、小売り、輸送を含む産業分野の世界的大手企業がDarktraceの自己学習型アプライアンスを使用しています。Darktraceは最先端の機械学習の専門家と政府のインテリジェンス エキスパートにより2013年に設立され本社は英国ケンブリッジと米国サンフランシスコにあり、オークランド、ボストン、シカゴ、ダラス、ロンドン、ロサンゼルス、ミラノ、ムンバイ、ニューヨーク、パリ、ソウル、シンガポール、シドニー、東京、トロントおよびワシントンDCに事務所を置いています。

お問い合わせ

電話: (03) 5456-5571

電子メール: japan@darktrace.com

www.darktrace.jp